CEH™

Certified Ethical Hacker Review Guide

IMPORTANTE

Este material es una traducción que se encuentra basada en el libro de estudio oficial para la certificación Ethical Hacking © escrito por Kimberly Graves y publicado por Sybex ©.

Este libro puede adquirirse en Sybex y en Amazon.

Tomando como base la mencionada publicación se genera la presente versión en traducción libre al idioma español y no pretende ser un reemplazo del original, el cual debe ser consultado ante cualquier duda.

Esta obra se entrega como está, sin ningún tipo de garantía y ni el autor ni el publicador se responsabilizan de su uso o abuso.

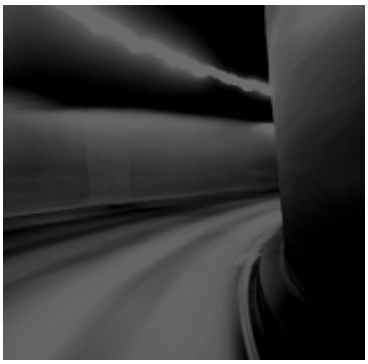
Nota: en este documento se evita el uso de la palabra “hacker” cada vez que se refiere a intrusiones no autorizadas, tomando como sinónimo la palabra “atacante”, por considerarlo el término más apropiado.

Idea y adaptación: Jorge Mieres
Publica: **www.segu-info.com.ar**
Versión: 1.0 - 20101012

Introducción al hacking ético, ética y legalidad

LOS OBJETIVOS CUBIERTOS EN ESTE CAPÍTULO SON:

- Ética y legalidad
- Terminología del hacking ético
- Fases involucradas en hacking ético
- Tipos de tecnologías hacking
- Las 5 etapas del hacking ético
- ¿Qué es el hacktivismo?
- Clases de hacker
- Habilidades necesarias para convertirse en un hacker ético
- ¿Qué es la investigación de vulnerabilidades?
- Conducta del hacker ético
- Implicancias legales del hacking
- Ley Federal de EE.UU. (18 U.S.C. 1029 y 1030)



La mayoría de las personas piensan que los hackers tienen habilidades y conocimientos extraordinarios que les permiten entrar a sistemas informáticos y obtener información valiosa.

El término hacker evoca la imagen de un joven genio de las computadoras quien escribe unos cuantos comandos en pantalla – y poof!, la computadora escupe de nuevo números de cuentas y otra información confidencial.

En realidad, un buen hacker sólo tiene que entender cómo trabajan los sistemas informáticos y cómo se utilizan las herramientas a fin de encontrar debilidades de seguridad. El reino de los hackers y la forma en que operan es desconocido para la mayoría de los profesionales de la seguridad.

El objetivo de éste capítulo es introducirlo en el mundo de los hackers y definir los términos que se pondrán a prueba en el examen de certificación CEH (*Certified Ethical Hacker*).

Terminología del hacking ético

Comenzar por ser capaz de entender y definir los términos es una parte muy importante de la responsabilidad de un CEH. En esta sección se discute una serie de términos con los cuales es necesario familiarizarse.

Una **amenaza** (*threat*) es un ambiente o situación que conduce a una potencial violación de la seguridad. El hacker ético busca y prioriza las amenazas de seguridad cuando realiza un análisis.

En seguridad informática, un **exploit** es una pieza de código que aprovecha un error, falla o vulnerabilidad de un sistema informático para ganar acceso no autorizado, escalar privilegios o realizar ataques de DoS (*denegación de servicio*).

En la clasificación de exploits, hay dos tipos:

Un **exploit remoto** funciona a través de una red y explota vulnerabilidades de seguridad sin ningún tipo de acceso previo a los sistemas vulnerables.

Un **exploit local** requiere acceso previo al sistema vulnerable para aumentar los privilegios.

El exploit es una forma de violación que define la seguridad de un sistema informático a través de una vulnerabilidad.

Una **vulnerabilidad** es la existencia de una falla que puede estar dada en el software, puede ser de tipo lógica, de diseño o un error de implementación que puede dar lugar a la ejecución de instrucciones o daño del sistema.

Un objetivo de evaluación (***target of evaluation***) es un sistema, programa o red que es objeto de un análisis de seguridad o de un ataque.

Un ataque ocurre cuando un sistema es comprometido a través de una vulnerabilidad. Muchos ataques son perpetrados a través de algún exploit. Un hacker ético utiliza herramientas para buscar sistemas que puedan ser vulnerables a través de alguna debilidad en el sistema operativo, en la configuración de la red o en los programas instalados en el sistema, para prevenir un ataque.

Además de conocer estos términos, también es importante identificar las diferencias entre un hacker ético y un atacante.

Diferentes tipos de tecnologías del hacking

Existen muchos métodos para localizar vulnerabilidades, ejecutar exploits y comprometer los sistemas informáticos. Troyanos, backdoors, sniffers, rootkits, exploits, desbordamientos de búfer (*buffer overflow*) e inyección de comandos SQL (*SQL injection*) son todas tecnologías que se pueden utilizar para atacar un sistema o una red.

Estas tecnologías y métodos de ataque son discutidos en los próximos capítulos. Muchos de ellos son tan complejos que todo un capítulo es dedicado a explicar el ataque y las tecnologías aplicables.

La mayoría de las herramientas de hacking explotan debilidades en alguno de los cuatro ámbitos siguientes:

Sistemas Operativos: Muchos administradores de sistemas instalan las plataformas con las configuraciones por defecto. Por lo tanto, en ese sistema operativo existen vulnerabilidades sin corregir.

Aplicaciones: Por lo general, las aplicaciones no se ponen a prueba para establecer potenciales vulnerabilidades en su código cuando los desarrolladores están escribiendo el software, esto puede dejar muchas fallas en la programación que un atacante puede explotar.

Código Shrink-wrap: La mayoría de los programas suelen tener opciones extras que el usuario común generalmente desconoce, y que pueden ser utilizadas para vulnerar el sistema. Un ejemplo de ello son las macros en Microsoft Word, que pueden permitir a un atacante ejecutar programas desde la aplicación.

Configuraciones por defecto: El sistema operativo también puede ser mal configurado o directamente no configurado con la finalidad de aumentar la facilidad de uso para los usuarios. Las configuraciones por defecto también pueden terminar en una vulnerabilidad o en un ataque.

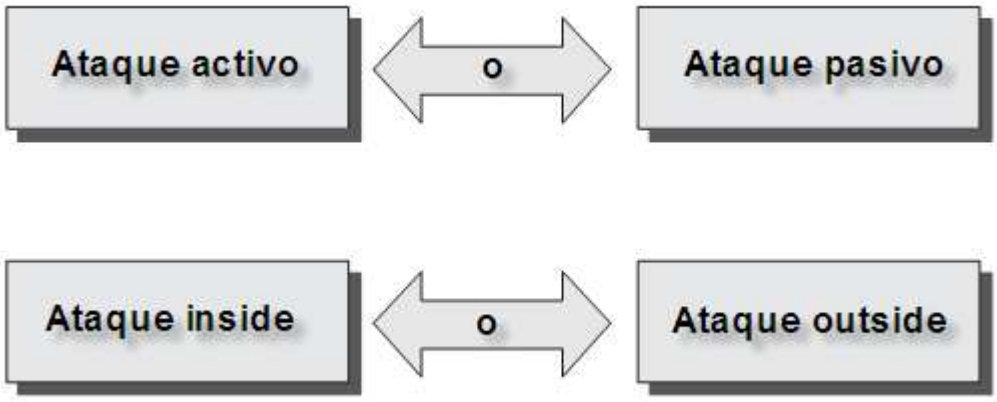
Este libro cubre todas estas tecnologías y herramientas de hacking en profundidad en los próximos capítulos. Es necesario comprender los tipos de ataques y los elementos básicos de la seguridad antes de aprender todas las tecnologías asociadas con un ataque.

Además de los diferentes tipos de tecnologías que un atacante puede utilizar, hay diferentes tipos de ataques que pueden ser clasificados en pasivos y activos.

Los ataques pasivos y activos son utilizados tanto sobre la infraestructura de la red como sobre la seguridad de cada nodo. Los ataques activos alteran el sistema o la red que están atacando, mientras que los ataques pasivos intentan obtener información del sistema. Los ataques activos afectan la disponibilidad, la integridad y la autenticidad de los datos; y los ataques pasivos son violaciones directas a la confidencialidad.

Además de las categorías de activos y pasivos, se clasifican en ataques insider (desde adentro) y ataques outsider (desde afuera). La figura 1.1 muestra la relación entre los ataques pasivos y los ataques activos, y los ataques insider y ataques outsider.

FIGURA 1.1 TIPOS DE ATAQUES



Un ataque procedente desde adentro del perímetro de seguridad de una organización es un ataque *insider* y por lo general es llevado a cabo por un "*insider*", una persona que obtiene o posee acceso a más recursos de lo esperado.

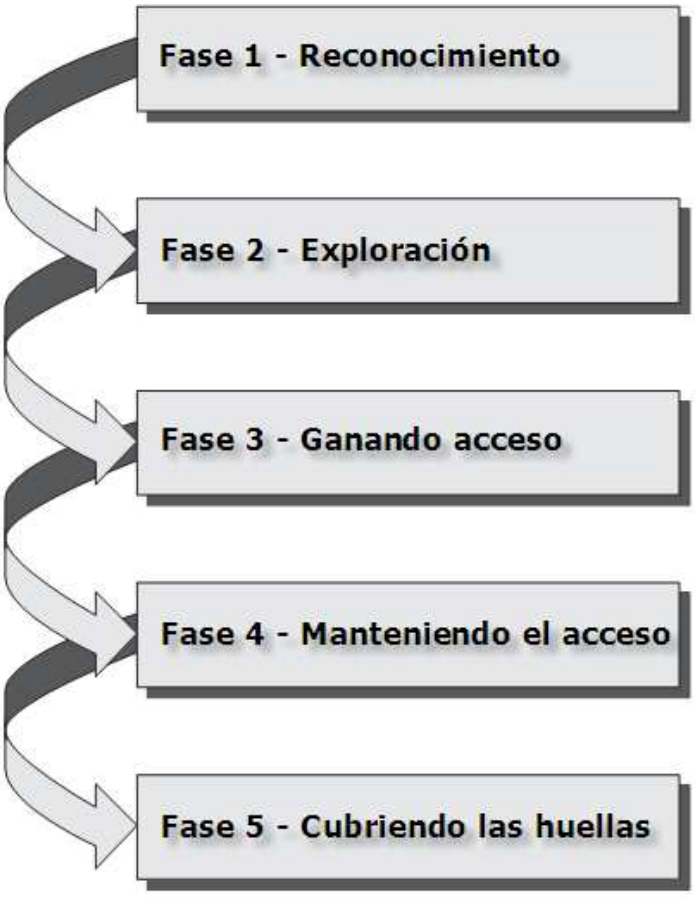
Cuando el ataque se origina desde una fuente que se encuentra fuera del perímetro de seguridad (exterior), como por ejemplos desde Internet o desde una conexión de acceso remoto, el ataque es del tipo *"outsider".*

La mayoría de las violaciones producidas a la seguridad de una red se originan desde el interior de la organización y por lo general son cometidas por empleados de la propia empresa o contratistas.

Fases involucradas en el Hacking Ético y listado de las cinco etapas del Hacking Ético

Un hacker ético sigue procesos similares a los de un atacante malicioso. Los pasos para obtener y mantener acceso al sistema informático son similares más allá de las intenciones del atacante. La figura 1.2 ilustra las cinco fases que los atacantes, en general, siguen para acceder a un sistema. Las siguientes secciones cubren estas cinco fases.

FIGURA 1.2 FASES DEL HACKING



Fase 1: Reconocimiento pasivo y reconocimiento activo (Reconnaissance)

El reconocimiento pasivo involucra la recolección de información con respecto a un potencial blanco sin tener conocimientos particulares de ese blanco. El reconocimiento pasivo puede ser tan simple como espiar un edificio para ver en qué momento entran los empleados y cuándo salen.

Sin embargo, generalmente esto se realiza buscando en Internet o buscando a través de los buscadores (generalmente Google) información sobre una persona o sobre alguna compañía. Este proceso es denominado "Recolección de información"

(*Information Gathering*). La Ingeniería Social (*Social Engineering*) y el basureo (*Dumpster Diving*) también son considerados métodos de recolección de información pasiva.

El Sniffing (olfatear) de red es otro de los métodos de reconocimiento pasivo y a través del cual es posible obtener información útil como direcciones IP, nombres convencionales, servidores o redes ocultas, y otros servicios disponibles en el sistema o en la red.

Realizar Sniffing en el tráfico de la red es similar a la construcción de la vigilancia: un atacante mira el flujo de datos para ver a qué hora se realizan las transacciones y hacia dónde va el tráfico de la red.

El reconocimiento activo implica el sondeo de la red para descubrir hosts, direcciones IP y servicios que se ejecutan en la red. Generalmente esto significa un mayor riesgo de ser detectado que en el reconocimiento pasivo y a veces es llamado "ratting the doorknobs".

El reconocimiento activo le puede brindar a un atacante información sobre las políticas de seguridad que se adoptan en el lugar, pero este proceso también aumenta la posibilidad de ser descubierto o al menos despertar sospechas.

Tanto el reconocimiento activo como el reconocimiento pasivo pueden conducir al descubrimiento de información útil que puede ser usada para realizar un ataque. Por lo general es fácil descubrir qué tipo de servidor web se esta utilizando y la versión de los sistemas operativos que emplea la empresa.

Esta información puede permitir encontrar una vulnerabilidad relacionada con la versión de ese sistema operativo y explotar la vulnerabilidad para obtener acceso al sistema.

Fase 2: Exploración (Scanning)

La fase de exploración implica la toma de la información descubierta durante la fase de reconocimiento y utilizarla para examinar la red. Las herramientas que un atacante puede emplear durante la fase de exploración pueden incluir port scanners, network mappers, sweepers y vulnerability scanners. Los atacantes buscan cualquier tipo de información que pueda ayudarles a perpetrar un ataque, como por ejemplo nombres de hosts, direcciones IP y cuentas de usuario.

Los métodos y herramientas utilizados en la fase de exploración son discutidos con mayor detalle en el capítulo 3 "*Exploración y enumeración*"

Fase 3: Ganando acceso (Gaining access)

Esta es la fase en la que el verdadero hacking tiene lugar. Las vulnerabilidades descubiertas durante las fases de exploración y reconocimiento ahora son explotadas para obtener acceso al sistema.

El método de conexión que el atacante utiliza para vulnerar el sistema pueden ser a través de una red de área local (LAN, ya sea por cable o inalámbrica), acceso físico a la

PC, desde Internet o fuera de línea. Los ejemplos incluyen desbordamiento de búfer (*Buffer Overflow*), denegación de servicio (*DoS – Denial of Service*) y secuestro de sesión (*Session hijacking*). En el mundo de los atacantes, ganar acceso se conoce como "posesión del sistema".

Fase 4: Manteniendo el acceso (Maintaining access)

Una vez que el atacante ha conseguido acceder al sistema, busca mantener ese acceso para futuras intrusiones y ataques. A veces, endurecen el sistema de otros atacantes o personal de seguridad para asegurar su acceso exclusivo a través de backdoors, rootkits y troyanos.

Cuando posee el sistema puede utilizarlo como base para ejecutar ataques adicionales. En este caso, el sistema informático comprometido es denominado computadora zombi.

Fase 5: Cubriendo las huellas (Covering tracks)

Una vez que el atacante han sido capaz de ganar y mantener el acceso al sistema, cubre las huellas para evitar ser detectado por el personal de seguridad, para poder seguir usando el sistema comprometido, para eliminar evidencias de la violación al sistema y/o para evitar acciones legales.

Es decir, trata de eliminar todos los rastros del ataque, como archivos de registro (*log*) o alarmas del Sistema de Detección de Intrusos (*IDS*). Ejemplos de actividades llevadas a cabo durante esta fase del ataque son la esteganografía (*steganography*), el empleo de protocolos de tunneling y la modificación de archivos de registro (*log*). Estos temas serán tratados en capítulos posteriores.

¿Qué es el hacktivismo?

El hacktivismo se refiere a la acción de ”hackear” por una causa. Por lo general estos ataques atienden a una agenda política o de índole social, y sus intenciones son utilizar sus conocimientos sobre hacking para enviar mensajes y ganar reputación sobre la causa que persiguen.

Muchos de estos personajes participan de actividades como el defacing de páginas webs, desarrollo de códigos maliciosos, DoS (*denegación de servicio*) y otros ataques agresivos con el ánimo de ganar notoriedad para sus causas.

Comúnmente, el objetivo del hacktivismo son las agencias gubernamentales, grupos políticos o cualquier otra actividad de grupos o personas que ellos consideren como malas o equivocadas.

"Por hacktivismo (un acrónimo de hacker y activismo) se entiende normalmente la escritura de código o la manipulación de bits para promover una ideología política, generalmente promoviendo políticas tales como la libertad de expresión, derechos humanos y ética de la información."

"Los actos del hacktivismo se llevan a cabo por personas que consideran que el uso apropiado el código puede tener efectos similares al activismo corriente o a la desobediencia civil. Pocas personas pueden escribir código, pero afecta a más personas."

"El término hacktivismo es controvertido. Algunos afirman que se acuñó para describir cómo la acción directa podría usarse en favor del cambio social al combinar la programación con el pensamiento crítico. Otros utilizan el término como sinónimo de actos maliciosos y destructivos que vulneran la seguridad de Internet como una plataforma tecnológica, económica y política.

Esencialmente la controversia refleja dos corrientes filosóficas divergentes dentro del movimiento hacktivista. Una corriente considera que los ataques cibernéticos maliciosos son una forma aceptable de acción directa. La otra corriente considera que toda protesta debe ser pacífica y sin violencia.

Algunas personas que se auto describen como hacktivistas se han dedicado a atacar y alterar sitios web por razones políticas, tales como ataques a sitios web del gobierno o de grupos que se oponen a su ideología. Otros, tales como Oxblood Ruffin se oponen activa y vocalmente al ataque y alteración de sitios web, así como a los ataques de denegación de servicio (DoS)."

"Dependiendo que quién utilice el término, el hacktivismo puede ser una forma políticamente constructiva de desobediencia civil anarquista o un gesto anti-sistema indefinido. Puede significar protesta política o anticapitalista."

Referencias
http://www.cultdeadcow.com/cDc_files/cDc-0384.php
http://www.securityfocus.com/news/11392

Extraído desde http://es.wikipedia.org.

Clases de hackers

Los hackers pueden ser divididos en tres grupos: white hats, black hats y grey hats (sombrero blanco, sombrero negro y sombrero gris respectivamente).

Por lo general, los hackers éticos se encuentran dentro de la categoría white hats (sombrero blanco) pero a veces ellos son ex grey hats que se han hecho profesionales de seguridad y que usan sus habilidades y conocimientos de una manera ética.

White hats: los white hats son los chicos buenos, los hackers éticos que utilizan sus habilidades de hacking con objetivos defensivos. Por lo general, los hackers de sombrero blanco son profesionales de seguridad con conocimientos de hacking y sobre cómo funcionan las herramientas de hacking, que utilizan sus conocimientos para localizar debilidades e implementar contramedidas.

Black hats: los black hats son los chicos malos, los hackers maliciosos o crackers quienes utilizan sus habilidades con fines ilegales, antimorales o propósitos maliciosos. Ellos violan y rompen la integridad de los sistemas de las máquinas remotas con intenciones maliciosas. Habiendo ganado acceso no autorizado, los hacker de sombrero negro destruyen datos útiles, niegan servicios a usuarios legítimos y, básicamente, causan problemas. Este tipo de hackers y crackers pueden ser fácilmente diferenciados de los hackers de sombrero blanco porque sus acciones son maliciosas. El cracker se distingue del hacker por sus valores morales, sociales y políticos.

Grey hats: los grey hats son los hackers que pueden trabajar de manera ofensiva o defensiva según las circunstancias y la situación. Esta es la línea que divide al hacker del cracker. Ambos son fuerzas poderosas en Internet y ambos permanecerán en esa situación, y algunas personas poseen habilidades que califican para ambas actitudes.

Además de estos grupos, hay quienes se auto-proclaman hackers éticos que se interesan en herramientas de hacking desde el punto de vista de la curiosidad. Ellos desean poner en evidencia los problemas de seguridad en un sistema informático o educar a las víctimas a fin de asegurar el sistema de manera correcta.

Estos hacker hacen favores a sus víctimas ya que, por ejemplo, si se descubre alguna debilidad en un servicio ofrecido por un banco, el hacker le está haciendo un favor al banco al advertir sobre dicha debilidad y ofrecerle la posibilidad de poder corregir la vulnerabilidad.

Desde un punto de vista más polémico, algunos consideran que el acto de hacking es contrario a la ética, al igual que "romper y entrar". Pero la creencia sobre que el hacking ético excluye de su filosofía a la destrucción, modera el comportamiento de quienes se ven a sí mismos como hackers benignos.

Según este punto de vista, puede ser una de las más altas formas de cortesía de hacking el hecho de irrumpir en un sistema para luego explicar de forma detallada al administrador de la red la manera exacta sobre cómo se hizo el ataque y la manera en que puede ser corregida la falla.

Este enfoque ha puesto en problemas legales a muchos hackers éticos. Hay que asegurarse de conocer bien la ley y sus responsabilidades legales cuando se practica la actividad del hacking ético.

Muchos de los que se auto-proclaman como hacker éticos están tratando de ingresar al ámbito de la seguridad informática como consultores. La mayoría de las empresas no ven favorablemente a alguien que aparece en la puerta de la empresa con datos confidenciales y ofertas para "arreglar" las vulnerabilidades de seguridad "por un precio". Las respuestas van desde "gracias por la información, vamos a solucionar el problema"; hasta llamar a la policía para detener al hacker ético auto-proclamado.

Ser capaz de identificar los tipos de hackers es importante, pero la determinación de las diferencias es también – si no más – importante. En secciones posteriores nos ocuparemos de esto.

Hackers éticos y crackers ¿Quiénes son?

Muchas personas se preguntan "¿puede ser ético un hacker?" Sí! Los hackers éticos suelen ser profesionales de seguridad que realizan pruebas de penetración en una red utilizando sus habilidades y conjunto de herramientas de hacking con fines defensivos y preventivos.

Es decir, un hacker ético es un profesional de seguridad que pone a prueba un sistema en busca de vulnerabilidades que pudieran comprometer la seguridad de ese sistema, utilizando las mismas herramientas que utilizaría un atacante malicioso. Cualquier equipo profesional puede aprender las habilidades del hacking ético.

Como se mencionó anteriormente, el término cracker describe un hacker que utiliza sus habilidades y el conjunto de herramientas de hacking para fines destructivos u ofensivos como la propagación de malware o para dejar fuera de servicio el sistema o la red (DoS).

Ya no sólo buscan divertirse sino que estos atacantes a veces son pagados para dañar reputaciones corporativas o robar información de tarjetas de crédito, mientras que al mismo tiempo frenan los procesos de negocio comprometiendo la integridad de la organización.

"Dentro de la cultura underground del Hacking , Hacker es toda aquella persona con elevados conocimientos informáticos independientemente de la finalidad con que los use. Mientras que Cracker es aquel individuo que se especializa en saltar las protecciones anticopia de software, de ahí el nombre crack para definir los programas que eliminan las restricciones en las versiones de demostración de software comercial."

Extraído desde http://es.wikipedia.org.

¿Qué hacen los hackers éticos?

Los hackers éticos están motivados por diferentes razones, pero su objetivo suele ser el mismo que el de los crackers: tratar de determinar lo que un intruso puede ver en un sistema o en una red, y qué se puede hacer con esa información. Este proceso que prueba la seguridad en un sistema o en una red se conoce como prueba de penetración o prueba de intrusión (*penetration test*).

Los atacantes penetran en los sistemas informáticos. Contrariamente al mito generalizado, no es un misterio ni una brillantez la manera en que acceden a un sistema sino más bien una tenaz persistencia y repetición de un conjunto de trucos que explotan debilidades comunes de los sistemas informáticos. En consecuencia, la mayoría de los crackers son atacantes mediocres.

Muchos hackers éticos detectan las actividades de los atacantes maliciosos como parte del equipo de seguridad de una organización encargada de la defensa contra las actividades del hacking malicioso. Cuando un hacker ético es contratado, pregunta a la organización qué se desea proteger, de quién y qué recursos la empresa está dispuesta a gastar para ganar seguridad.

Objetivos que los atacantes tratan de alcanzar

La seguridad consta de cuatro elementos básicos:

- Confidencialidad
- Autenticidad
- Integridad
- Disponibilidad

El atacante tiene por vocación explotar las vulnerabilidades de un sistema o de una red para encontrar una o más debilidades de los cuatro elementos de seguridad. En el desempeño de una ataque de DoS, se ataca la disponibilidad de los elementos del sistema o de la red.

Aunque un ataque de DoS puede adoptar varias formas, el objetivo principal es utilizar recursos del sistema o ancho de banda, y fundamentalmente, se trata de enviar una avalancha de mensajes al sistema víctima para forzar el cierre del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema.

Aunque los ataques de denegación de servicio centran sus objetivos en los medios de comunicación, en realidad la meta de esos ataques tienen muchas víctimas – el objetivo final y los sistemas de control de intrusos.

El robo de información, como el robo de contraseñas u otros datos viajan en texto claro a través de redes confiables, esto es un ataque a la confidencialidad, ya que permite que otra persona que no es el destinatario tenga acceso a los datos.

Los dispositivos que almacenan la información como las computadoras portátiles, los discos y las cintas de copias de seguridad siempre están en peligro. Estos dispositivos son propiedad de la compañía y están cargados de información confidencial que puede ser necesaria para que un atacante conozca las medidas de seguridad de una organización.

Los ataques **bit-flipping** son considerados ataques a la integridad de la información, porque los datos son alterados durante el tránsito o en el resto de los sistemas informáticos, por lo tanto, los administradores del sistema no son capaces de verificar que los datos llegaron como pretendían el verdadero remitente.

Un ataque bit-flipping es un ataque dirigido al algoritmo criptográfico: mientras la información viaja, el atacante realiza cambios en los bits del texto cifrado, como una manera de dar lugar a un previsible cambio del texto, aunque el atacante no conozca el texto en sí mismo.

Este tipo de ataque no es directamente contra el sistema de cifrado pero es en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utilizan cifrado.

El ataque es especialmente peligroso cuando el atacante sabe el formato del mensaje. Cuando un ataque bit-flipping es aplicado a las firmas digitales, el atacante puede ser capaz de cambiar el texto de un pagaré que declara "Le debo U$S 1.000" por otro que diga "Le debo U$S 10.000".

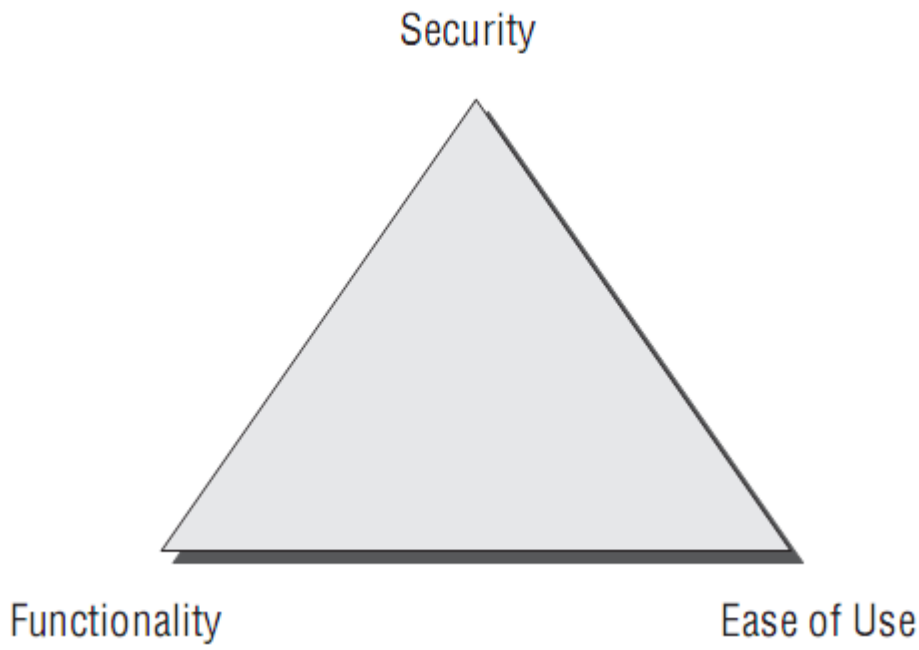
Los ataques de suplantación de dirección MAC (MAC Address Spoofing) atacan la autenticación ya que permiten que un dispositivo no autorizado se conecte a la red aunque exista implementado un filtro de direcciones MAC en el lugar, como en una red inalámbrica. Pero la suplantación de direcciones MAC de una estación inalámbrica legítima puede ser utilizada por un intruso para cambiar la identidad de aquella estación y así acceder y utilizar la red.

Triángulo de seguridad, funcionalidad y facilidad de uso

Como medida de seguridad profesional, es difícil lograr un justo equilibrio entre la adición de barreras de seguridad para evitar un ataque y permitir que el sistema siga siendo funcional para todos los usuarios.

El **triángulo de seguridad, funcionalidad y facilidad de uso** es una representación del equilibrio entre la seguridad y la funcionalidad del sistema y la facilidad de uso para los usuarios (ver figura 1.3). En general, cuando la seguridad aumenta, la funcionalidad del sistema y la facilidad de uso para los usuarios disminuyen.

FIGURA 1.3 TRIÁNGULO DE SEGURIDAD, FUNCIONALIDAD Y FACILIDAD DE USO



En un mundo ideal, los profesionales de seguridad desearían tener el más alto nivel de seguridad en todos los sistemas, sin embargo, a veces esto no es posible. Demasiadas barreras de seguridad impiden la funcionalidad del sistema haciendo que sea difícil para los usuarios utilizarlo.

Supongamos que, para poder entrar a la oficina en el trabajo, hay que pasar primero por un guardia que controla la entrada al estacionamiento para verificar su número de matrícula, a continuación mostrar una tarjeta de identificación cuando se ingresa al edificio, luego, utilizar un código de acceso para poder subir al ascensor, y por último, utilizar una llave para abrir la puerta de la oficina.

Usted podría sentir que los controles de seguridad son muy estrictos! Cualquiera de estos controles puede causar que usted se detenga y, en consecuencia, se pierda una importante reunión - por ejemplo, si se ha olvidado la clave o la tarjeta de identificación para acceder al edificio, subir al ascensor, o para la puerta de la oficina.

Habilidades requeridas para convertirse en un hacker ético

Para que un hackers éticos pueda estar un paso por delante de los atacantes maliciosos deben ser expertos en sistemas informáticos y estar muy familiarizados con la programación informática, la creación de redes y sistemas operativos. Conocimiento profundo altamente orientado a plataformas como Windows y Unix también es un requisito.

La paciencia, la persistencia y la perseverancia son importantes cualidades que muchos hackers poseen debido a la cantidad de tiempo y el nivel de concentración necesario que requieren para realizar la mayoría de los ataques, comprometer los sistemas y obtener sus frutos.

La mayoría de los hackers éticos tienen conocimiento de las áreas de seguridad o relacionadas a ella, pero no necesariamente tienen un fuerte control sobre las contramedidas que pueden prevenir los ataques. Los siguientes capítulos de este libro se ocuparán tanto de las vulnerabilidades como de la lucha para prevenir ciertos tipos de ataques.

¿Qué es la investigación de vulnerabilidades?

La investigación de vulnerabilidad es el proceso que permite descubrir las vulnerabilidades y debilidades de diseño que podrían conducir al ataque de un sistema. Existen varios sitios web y herramientas que ayudar al ética hacker en el mantenimiento de un listado actualizado de vulnerabilidades y posibles exploits para sus sistemas o redes.

Es esencial que un administrador de sistemas se mantenga actualizado sobre los últimos códigos maliciosos, exploits y otras amenazas comunes con el fin de proteger adecuadamente los sistemas y la red. Además, al familiarizarse con las amenazas más recientes, un administrador puede aprender a detectar, prevenir y recuperarse de un ataque.

Describiendo los caminos que conducen al hacking ético

El hacking ético es llevado a cabo de una manera organizada y estructurada, por lo general como parte de una prueba de intrusión o de una auditoria de seguridad. La profundidad y la amplitud de los sistemas y las aplicaciones que deben someterse a pruebas, en la mayoría de los casos están determinadas por las necesidades y las preocupaciones del cliente. Muchos hackers éticos son miembros de un equipo de seguridad.

Los siguientes pasos son un marco para la realización de una auditoria de seguridad en una organización:

1. Hablar con el cliente y discutir las necesidades que se abordarán durante la prueba.

2. Preparar y firmar con el cliente un acuerdo de no divulgación (NDA) de los documentos.

3. Organizar un equipo de hacking ético y preparar un calendario para la realización de pruebas.

4. Coordinar la prueba.

5. Analizar los resultados de las pruebas y preparar un informe.

6. Presentar el informe al cliente.

Las pruebas de penetración y las auditorias de seguridad se examinan en profundidad en la certificación de "Licencia del Consejo de prueba de penetración" (LPT) de EC-Council.

Creación de un plan de evaluación de la seguridad

Muchos hackers éticos actuando en el rol de profesionales de seguridad usan sus habilidades para llevar a cabo evaluaciones de seguridad o pruebas de penetración. Estas pruebas y evaluaciones tienen tres fases, en general, ordenadas de la siguiente manera:

La fase de preparación consiste en un acuerdo formal entre la ética del hacker y la organización. Este acuerdo debería incluir todo el ámbito de la prueba, los tipos de ataques (insider y outsider) que se realizarán y las pruebas de los tipos white, black o grey box.

Durante la fase de realización de la evaluación de seguridad, las pruebas se realizan después de que el que llevará a cabo la prueba prepare un reporte formal sobre las vulnerabilidades encontradas y otras conclusiones. Los resultados se presentan a la organización en la fase de conclusión, junto con todas las recomendaciones para mejorar la seguridad.

Tipos de hacking ético

Los hackers éticos pueden utilizar diferentes métodos para violar la seguridad de una organización durante un ataque simulado o durante una prueba de intrusión (penetration test). Los métodos más comunes son:

Red remota: intenta simular una intruso ejecutando un ataque a través de Internet. El hacker ético intenta romper o encontrar una vulnerabilidad desde afuera (outside) de las defensas de la red, como vulnerabilidades en el firewall, el proxy o en el router.

Red dial-up remota: trata de simular una intrusión ejecutando un ataque contra el pools de módems de los clientes. El *war dialing* es el proceso de repetición de marcación para encontrar un sistema abierto y es un ejemplo de un ataque de ese tipo.

Red local: simula a alguien con acceso físico ganando acceso adicional no autorizado utilizando la red local. El hacker ético debe ganar acceso directo a la red local con el fin de llevar a cabo este tipo de ataque.

Equipo robado: simula el robo de un recurso crítico de información como lo es una computadora portátil que es propiedad de un empleado. Información como nombres de usuario, contraseñas, configuraciones de seguridad y tipos de cifrado pueden ser obtenidos al robar una computadora portátil.

Ingeniería Social: intenta comprobar la integridad de los empleados de la organización utilizando el teléfono o a través de una comunicación cara a cara para obtener información que pueda ser útil para cometer un ataque. Los ataques de Ingeniería Social pueden ser utilizados para la obtención de nombres de usuario, contraseñas y otras medidas de seguridad de la empresa.

Entrada física: constituyen intentos de comprometer a la organización física de los locales. Una hacker ético que logra el acceso físico a la organización puede plantar virus, troyanos, rootkits o keyloggers por hardware (dispositivo físico utilizado para registrar las pulsaciones del teclado) directamente sobre los sistemas de la red.

Tipos de pruebas

Cuando se realizan pruebas de seguridad o pruebas de intrusión, un hacker ético lleva a cabo uno o más métodos de pruebas sobre el sistema. Cada tipo simula un atacante con diferentes niveles de conocimiento sobre la organización objetivo. Estos tipos son los siguientes:

Black Box (Caja Negra): implica la realización de una prueba y evaluación de la seguridad sin conocimientos previos sobre la infraestructura de la red o sobre el sistema que es sometido a prueba. La prueba simula el ataque malicioso desde fuera del perímetro de seguridad de la empresa.

White Box (Caja Blanca): consiste en realizar una evaluación y una prueba de la seguridad con total conocimiento de la infraestructura de la red como, por ejemplo, si se tratase de un administrador de red.

Grey Box (Caja Gris): implica la realización de una prueba para evaluar la seguridad y otras pruebas internas. Esta prueba examina el grado de acceso de las personas con información privilegiada dentro de la red.

Reporte de hacking ético

El resultado de una prueba de penetración de la red o de una auditoria de seguridad es un informe de hacking ético. En este informe se detallan los resultados de las actividades del hacking, los tipos de pruebas realizadas y los métodos de hacking utilizados.

Estos resultados son comparados contra los trabajos previstos en la fase de evaluación de la seguridad. Cualquier vulnerabilidad identificada es detallada junto a las contramedidas que se sugieren. Este documento suele ser entregado a la empresa en formato de copias impresas por razones de seguridad.

Los detalles del informe de hacking ético deben ser mantenidos en total confidencialidad ya que contiene información sobre los riesgos de seguridad y las vulnerabilidades de la empresa. Si este documento cae en malas manos, los resultados podrían ser desastrosos para la organización.

Implicancias legales del hacking

Un hacker ético debe conocer las penas que sufre el hacking no autorizado en un sistema. Las actividades relacionadas con el hacking ético de una red, una prueba de penetración o de una auditoria de seguridad deben comenzar a realizarse mediante un documento legal firmado que le da permiso expreso al hacker ético para llevar a cabo las actividades de hacking en la organización que es objeto de prueba. Los hackers éticos necesitan ser prudente con sus habilidades de hacking y reconocer las consecuencias que implica el mal uso de esos conocimientos.

En términos generales, los delitos informáticos pueden clasificarse en dos categorías: delitos cometidos por computadoras y delitos donde la computadora es el objetivo.

Las dos leyes más importantes de EE.UU. en relación a los delitos informáticos se describen en la siguiente sección. Aunque el examen CEH es de alcance internacional, asegúrese de familiarizarse con estos dos estatutos estadounidenses y las penas por el hacking. Recuerde, la intención no es crear un hacker por encima de las leyes, de hecho un hacker ético puede ser procesado por violar estas leyes.

El *Cyber Security Enhancement Act of 2002* condena a cadena perpetua a los hackers que "temerariamente" ponen en peligro la vida de los demás. Usuarios malintencionados que crean una situación de peligro a la vida atacando las redes informáticas de los sistemas de transporte, empresas de energía o de otros servicios públicos o de empresas de servicios públicos pueden ser procesados en virtud de la presente ley.

Ley Federal de USA (18 U.S.C. § 1029 y 1030)

El Código de los EE.UU. clasifica y define las leyes de los Estados Unidos por títulos. El Título 18 detalla "Delitos y procedimiento penal". La sección 1029 "Fraude y actividades relacionadas en conexión con dispositivos de acceso," establece que quien produce, vende o utiliza dispositivos de acceso falsificados o instrumentos de telecomunicaciones con la intención de cometer fraude y obtener servicios o productos con un valor de U$S 1000, infringe la ley. La sección 1029 tipifica como delito el uso indebido de contraseñas de computadoras y otros dispositivos de acceso como las tarjetas token.

La sección 1030, "Fraudes y actividades relacionadas con conexión de computadoras," prohíbe el acceso a computadoras protegidas sin autorización para causar daño. Esta ley tipifica como delito la propagación de virus, gusanos y el acceso a los sistemas informáticos por personas no autorizadas.

"En los Estados Unidos, existen leyes federales que protegen contra el ataque a computadoras, uso ilegítimo de contraseñas, invasiones electrónicas a la privacidad y otras transgresiones.

Las dos leyes Federales de EEUU más importantes utilizadas por los jueces Federales para perseguir a los delincuentes informáticos son: 18 USC, CAPÍTULO 47, SECCIÓN 1029 Y SECCIÓN 1030, de 1994 que modificó al Acta de Fraude y el Acta Federal de Abuso Computacional de 1986.

El Pronunciamiento sobre Abuso y Fraude Informático de 1986, es la principal pieza legislativa aplicable a la mayoría de los delitos informáticos, aunque muchas otras leyes pueden ser usadas para perseguir diferentes tipos de delitos informáticos.

El pronunciamiento fue modificado con el Título 18 USA, Código 1030. También complementó a la Ley de Privacidad de las Comunicaciones Electrónicas de 1986, que dejó fuera de la ley el acto de interceptar comunicaciones electrónicas. Las Modificaciones de la Ley de Abusos Informáticos de 1994 amplió la Ley de 1986 al acto de transmitir virus y otra clase de códigos maliciosos.

Con la finalidad de eliminar los argumentos hiper-técnicos acerca de qué es y que no es un virus, un gusano, un troyano, etcétera; y en que difieren entre ellos, el acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, a las redes, a la información, a los datos o programas (18 U.S.C. Sec.1030 (a) (5) (A)."

En general, un delito informático quebranta las leyes federales cuando entra en alguna de las siguientes categorías:

- *Implica el compromiso o el robo de información de defensa nacional, asuntos exteriores, energía atómica u otra información restringida.*

- *Involucra a una computadora perteneciente a departamentos o agencias del gobierno de los Estados Unidos.*
- *Involucra a una entidad bancaria o cualquier otra clase de institución financiera.*
- *Involucra comunicaciones interestatales o con el extranjero.*
- *Afecta a gente o computadoras en otros países o estados.*

Sección 1029

La Sección 1029 prohíbe el fraude y cualquier actividad relacionada que pueda realizarse mediante el acceso o uso de dispositivos falsificados como PINs, tarjetas de crédito, números de cuentas y algunos tipos más de identificadores electrónicos.

Las nueve áreas de actividad criminal que se cubren en la Sección 1029 están listadas abajo. Todas "requieren" que el delito implique comercio interestatal o con el extranjero.

1. Producción, uso o tráfico de dispositivos de acceso falsificados.

2. Uso u obtención sin autorización de dispositivos de acceso para obtener algo de valor totalizando $1000 o más, durante un periodo de un año.

3. Posesión de 15 o más dispositivos de acceso no autorizados o falsificados.

4. Fabricación, tráfico o posesión de equipo de fabricación de dispositivos de acceso ilegales.

5. Realización de transacciones con dispositivos de acceso pertenecientes a otra persona con el objetivo de obtener dinero o algo de valor totalizando $1000 o más durante un periodo de un año.

6. Solicitar a una persona con el objetivo de ofrecerle algún dispositivo de acceso o venderle información que pueda ser usada para conseguir acceso a algún sistema.

7. Uso, producción, tráfico o posesión de instrumentos de telecomunicación que hayan sido alterados o modificados para obtener un uso no autorizado de un servicio de telecomunicaciones.

8. Uso, fabricación, tráfico o posesión de receptores-escaneadores o hardware o software usado para alterar o modificar instrumentos de telecomunicaciones para obtener acceso no autorizado a servicios de telecomunicaciones. Esto también incluye los escaners que mucha gente usa para interceptar llamadas de teléfonos celulares (hammers).

9. Hacer creer a una persona que el delincuente es un miembro de su compañía de tarjeta de crédito o su agente para obtener dinero o realización de transacciones hechas con un dispositivo de acceso y viceversa (tratar de hacer creer a la compañía de crédito que se trata de la persona legítima).

La Sección 1030

18 USC, Capítulo 47, Sección 1030. Como parte de la Ley sobre Abuso y Fraude Informático de 1986, prohíbe el acceso no autorizado o fraudulento a computadoras gubernamentales, y establece diversas condenas para esa clase de accesos. Esta ley es una de las pocas piezas de legislación federal únicamente referidas a computadoras.

Bajo la Ley de Abuso y Fraude Informático, el Servicio Secreto americano (CIA) y el FBI tienen jurisprudencia para investigar los delitos definidos en este decreto. Las seis áreas de actividad criminal cubiertas por la Sección 1030 son:

1. Adquisición de información restringida relacionada con defensa nacional, asuntos exteriores o sobre energía nuclear con el objetivo o posibilidad de que sean usados para dañar a los Estados Unidos o para aventajar a cualquier otra nación extranjera.

2. Obtención de información en un registro financiero de una institución fiscal o de un propietario de tarjeta de crédito; o de información de un cliente en un archivo de una agencia de información de clientes.

3. Atacar un ordenador que sólo corresponda ser usado por algún departamento o agencia del gobierno de los EEUU, para el caso de que no sólo puede ser usada por esta agencia, atacar una computadora usada por el gobierno en el que la intrusión producida afecte el uso que el gobierno hace de este.

4. Promover un fraude accediendo a una computadora de interés federal y obtener algo de valor, a menos que el fraude y la cosa obtenida consistan solamente en el uso de dicha computadora.

5. A través del uso de una computadora utilizada en comercio interestatal, transmitir intencionalmente programas, información, códigos o comandos a otro sistema informático. Existen dos situaciones diferentes:

> *A.- En esta situación (I) la persona que realiza la transmisión está intentando dañar otra computadora o provocar que no se permita a otras personas acceder a ella; y (II) la transmisión se produce sin la autorización de los propietarios o usuarios de las computadoras, y causa $1000 o más de pérdidas, o modifica o perjudica, o potencialmente modifica o altera un examen o tratamiento médico. Pena con intento de dañar: Multa y/o hasta 5 años de cárcel. Hasta 10 años si se reincide.*
>
> *B.- En esta situación, (I) la persona que realiza la transmisión no intenta hacer ningún daño, pero actúa imprudentemente despreciando el riesgo que existe de que la transmisión causara daño a los propietarios u operadores de los ordenadores y provoca $1000 o más de pérdidas, modifica o potencialmente modifica un examen o tratamiento médico. Pena por actuación temeraria: multa y/o hasta 1 año de cárcel.*

6. Promover el fraude traficando con contraseñas o información similar que haga que se pueda acceder a una computadora sin la debida autorización.

Para la Sección 1030, una computadora de interés federal tiene las siguientes características:

1. Una computadora que es exclusivamente para el uso de una institución financiera o del Gobierno de los EEUU, o si su uso no está restringido a lo anterior, usado por una institución financiera o el gobierno de los EEUU en el que el ataque afecte negativamente al servicio que está desarrollando en esas instituciones.

2. Una computadora de los dos o más que hayan sido usados para cometer el ataque, no estando todos ellos en el mismo Estado. Las disposiciones citadas se complementan con los siguientes instrumentos: ***18.U.S.C. 875 Interstate Communication Including Threats, kidnapping, Ransom, extortion 18 U.S.C. 1343 Fraud by wire, radio or television 18 U.S.C. 1361 Injury to Goverment Property 18 U.S.C. 1362 Government Communication systems 18 U.S.C. 1831 Economic Espionage Act 18 U.S.C. 1832 Trade Secrets Act.***

Extraído desde http://www.aadat.org/delitos_informaticos20.htm

Temas esenciales

Entender la terminología esencial del hacking. Deben asegurarse de estar familiarizados con los términos, pudiendo definir sin problemas los conceptos de amenaza, exploit, vulnerabilidad, blanco de evaluación y ataque.

Entender la diferencia entre hacker ético y cracker. Los hackers éticos son profesionales de seguridad que actúan defensivamente. Los crackers son usuarios malintencionados que optan por causar daños sobre un sistema víctima.

Conocer las clases de hackers. Es de vital importancia conocer las diferencias entre hackers del tipo Black Hat, White Hat y Grey Hat. Básicamente saber quiénes son los chicos buenos y quiénes son los chicos malos en el mundo del hacking.

Conocer las fases del hacking. El reconocimiento pasiva y el reconocimiento activo, la exploración, ganar el acceso, mantener el acceso y cubrir las huellas (reconnaissance, scanning, gaining access, maintaining access y covering tracks respectivamente) son las cinco fases del hacking. Conocer el orden de las etapas y lo que ocurre en cada una de ellas.

Ser consciente de los tipos de ataques. Entender las diferencias entre ataques activos y ataques pasivos, y ataques Insider y Outsider. La capacidad de ser detectado es la diferencia entre el ataque pasivo y el activo. La ubicación del atacante es la diferencia entre ataque Insider y ataque Outsider.

Conocer los tipos de hacking ético. Los hackers pueden atacar la red desde una red remota, desde una red dial-up remota, desde una red local, por medio de Ingeniería Social, robando algún equipo o accediendo físicamente.

Entender los tipos de pruebas de seguridad. Los hackers éticos pueden poner a prueba una red a través de técnicas de prueba como Black Box, White Box o Grey Box.

Conocer el contenido de un reporte de hacking ético. Un reporte de hacking ético contiene información sobre las actividades de hacking que se realizan sobre la red o sobre el sistema, las vulnerabilidades descubiertas y las contramedidas que deberían aplicarse para corregir los puntos vulnerables.

Conocer las implicaciones jurídicas involucradas en el hacking. La *Cyber Security Enhancement Act of 2002* puede ser utilizada para perseguir a los hackers éticos que imprudentemente ponen en peligro la vida de los demás.

Ser consciente de las leyes y la pena aplicable ante una intrusión. El Título 18 y las secciones 1029 y 1030 del Código de los EE.UU. tipifican y establecen las sanciones por hacking sin importar cual haya sido la intención.